AMENDMENTS TO THE SPECIFICATION

Please cancel the previous Abstract, and add the new Abstract as follows:

ABSTRACT

The present invention relates to a method for enabling strong mutual authentication between two computers in a communication system. A user from a client attempts to gain access to a server. The server transmits a first key encrypted by a second key to the client and a second key encrypted by a user's private key to a verifier. The verifier uses the user's login information to obtain the user's private key, which the verifier uses to obtain the second key. The verifier transmits the second key to the client and the client decrypts the first key with the second key. The client then transmits the second key encrypted by the first key to the server. If the received second key is the same as the generated second key, the client is authenticated to the server.